ARGEO PAUL CELLUCCI
Governor

WILLIAM D. O'LEARY
Secretary

HOWARD K. KOH, MD, MPH
Commissioner

The Commonwealth of Massachusetts

Executive Office of Health and Human Services
Department of Public Health
Division of Health Care Quality
10 West Street, Boston Ma 02111
617-753-8000

CIRCULAR LETTER: DHCQ-1-99-387

TO: Hospital Administrators

FROM: Paul I. Dreyer, Ph.D., Director

DATE:

RE: Year 2000 Compliance

The attached material is being sent to you to bring to your attention the Department's concern about the potential impact of the infamous "Year 2000" (Y2K) problem. The services provided by your hospital are essential to the well being of thousands of Massachusetts residents. Many important aspects of hospital operations are tied to computerized functions. As the agency responsible for licensing hospitals, it is in our mutual interest that we seek assurance from you that your mission-critical (defined on the next page) and other essential operations will continue uninterrupted.

If you are not already intimately familiar with the potential scope of Y2K issues, you should note that the operations of most businesses today involve the use of computer technology both directly and indirectly. The Y2K problem can involve not just "computers", but all equipment containing "embedded" computer chips in biomedical or environmental equipment (e.g. IV pumps in health care.) It is prudent to insure that all mission critical devices will function properly so that business and service continuity can be assured as the calendar advances.

The steps itemized in the attached certification statement and review documents, while comprehensive, have been designed as basic as possible, following a review approach used by Commonwealth agencies, businesses and other organizations already engaged in addressing this complex issue. Please see that the appropriate persons in your hospital prepare the answers.

If you have questions, contact Larry Bohan at (61) 753-8000. Please send the completed forms and worksheets to:

Rose Silva
Department of Public Health
Division of Health Care Quality
10 West Street, Boston Ma 02111

Thank you for your prompt attention to this very important matter.

Hospital Name: _____

CEO /President: _____

The undersigned confirm that the hospital named above is actively working to achieve Year 2000 compliance.

Definitions:

- **Compliance**. The Massachusetts Government User Group has defined Year 2000 compliance as follows:

  "Year 2000 compliant means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, Year 2000 compliant information technology, when used in combination with other information technology (IT), shall accurately process date/time data if the other information technology properly exchanges date/time data with it."

- **Mission critical systems** We are defining a mission critical system as an IT, biomedical equipment or other type of embedded system:

  - Which directly impact the health, safety, or livelihood of clients/patients.
  - Which directly impact the revenue of the enterprise.
  - Whose loss would severely jeopardize hospital delivery of services.

- **Essential systems**. We define an essential system as an IT, biomedical equipment or embedded system whose loss would cause a disruption of some hospital services but the hospital could still deliver primary services.

The attached documents indicate the hospital's status at this time.

_____ _____

Signature of Hospital Executive Date

Phone ( ) ____ - _____ Fax ( ) ____ - _____

E-Mail _____

The following items identify aspects of achieving readiness for the date transitions. A "no" on any item should generate activity within the hospital.

1. Hospital has completed **an inventory of IT systems and or embedded systems** at all locations. The inventory includes third party components such as hardware, microprocessor-based devices, system software, and application software.
   Yes ____ No ____ Sched. Completion Date: _____ NA ____

2. For each item in the inventory, hospital has defined **criticality** (mission critical, essential, other), assessed Y2K **exposure**, and determined a **Y2K strategy** (e.g., upgrade, retire, remediate, replace).
   Yes ____ No ____ Sched. Completion Date: _____ NA ____

3. All **centralized hardware platforms** (database servers, etc) have been checked (firmware, operating systems, and system support software, and third party software) and are compliant.
   Yes ____ No ____ Sched. Completion Date: _____ NA ____
   Most manufacturers have Internet sites listing tested and compliant products

4. All **PCs, including notebooks**, have been checked (BIOS, operating system, and third party software) and are compliant.
   Yes ____ No ____ Sched. Completion Date: _____ NA ____
   Most manufacturers have Internet sites listing tested and compliant products.

5. All **Infrastructure -- LANs and WANs** (servers, network software, messaging systems, hubs, routers, and other network devices) has been checked and found compliant.
   Yes ____ No ____ Sched. Completion Date: _____ NA ____
   Most manufacturers have Internet sites listing tested and compliant products

6. All **Biomedical equipment** at all locations has been checked for **embedded devices** and is compliant.
   Yes ____ No ____ Sched. Completion Date: _____ NA ____

7. **Non-medical facility equipment** (e.g. elevators, HVAC systems, lighting, alarm systems) has been checked for embedded devices and is compliant.
   Yes ____No ____ Sched. Completion Date: _____ NA ____

8. All **phone and voice mail systems** and related telecommunications devices and software have been checked and are compliant.
   Yes ____No ____ Sched. Completion Date: _____ NA ____

9. All major **suppliers of mission-critical items** have been contacted for compliance status.
   Yes ____ No ____ Sched. Completion Date: _____ NA ____

GLOSSARY

BIOS – This is "tech-talk" for "Basic Input and Output System". It refers to a special-purpose processor in all computers. The function of this chip is to manage the movement of data into and out of the computer system. The BIOS is "built in" and often converts the timing clock's pulses into a real-time date and time. Obviously, if it was constructed with a two-digit year, it will be wrong from 1/1/2000 forward.

Embedded Chips -- Special purpose digital processors that are built in to equipment of all kinds. Sometimes these do not use or contain "dates", but almost always have a digital clock that is used to trigger the execution of built-in instructions. In many circumstances the actual results are "unpredictable".

Essential systems – Systems or pieces of equipment whose loss, while not "mission critical", would impede efficient operations or require a 'work-around'.

Firmware – The instructions 'built in" to hardware components (E.g. BIOS).

Hardware -- Computer (or other) equipment – distinguished from software.

Mission Critical systems – Refers to the mission of the hospital, and the role of a system or piece of equipment within it. If a failure of technology – embedded chips or an information system – would cripple operations or functions that are fundamental to the hospital's mission, it qualifies as "mission critical". [Examples: IV Pumps, defibrillators, medication dispensing systems, EKGs, EEGs and other monitoring devices].

Mission Critical Items – In thinking about suppliers, consider those who deliver such things as medical supplies, food (for residential or other food-service programs), pharmaceuticals, or sterile surgical supplies.

Software – Groups of instructions that direct the computer's processing components in accomplishing a set of tasks on behalf of an enterprise. The term includes operating systems (E.g. Windows 95), utilities such as communication software and e-mail, productivity packages like word processing and spreadsheets, and applications developed particularly for hospitals.

Testing – Verifying by experimentation that hardware components, or remediated software, will correctly process dates following the beginning of the next century. Information and aids for testing are available on the Commonwealth's Y2K website -- http://www.magnet.state.ma.us/y2k/

Y2K – A shorthand "tag" for the array of potential difficulties that could arise where Information Systems or their components (computer hardware, operating systems, application software) and automated functions such as elevators, phone systems, using "embedded chips" – special purpose processors. The source of problems is the historic practice of creating processing hardware "clocks" with space for only two digits indicating the year. On January 1, 2000, the "year" in such a "clock" – or date-fields in a software program – would contain "00". In some cases this would be slightly confusing to human users, but acceptable. In other instances, such as aging calculations, sorting by dates, 'date-stamping', or triggering time-based actions whose results could be catastrophic.

WORKSHEETS

Hospital Mission Critical Systems (including non-IT, end-user, and PC applications):

System	Actual Date Compliant Version in Production	Sched. Date Compliant Version in Production	System Compliance Status (Part 2) Attached

Hospital Essential Systems (including non-IT, end-user, and PC applications):

System	Actual Date Compliant Version in Production	Sched. Date Compliant Version in Production	System Compliance Status (Part 2) Attached

Business Continuity Options:

Service Disruption Description	Contingency/Recovery Description	Trigger Duration*	Resources Required for Implementation		
			Cost	Staffing	Equipment/ Facilities

* The maximum duration of the service disruption that would necessitate implementation of the contingency.

Business continuity planning should focus on Mission Critical and, to some extent, Essential systems and equipment which will have a direct impact on patient health care, and should identify alternative means for accomplishing the goals of a failed entity. Some downtime can be tolerated for most functions. The determination of how much time, and how long the alternative method can be expected to work adequately are keys to effective contingency planning.